UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

PASCAL ABIDOR, NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS, NATIONAL PRESS PHOTOGRAPHERS ASSOCIATION,

Plaintiffs,

v.

JANET NAPOLITANO, in her official capacity as Secretary of the U.S. Department of Homeland Security; ALAN BERSIN, in his official capacity as Commissioner, U.S. Customs and Border Protection; JOHN T. MORTON, in his official capacity as Assistant Secretary of Homeland Security for U.S. Immigration and Customs Enforcement,

Defendants.

COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

Case No.

CV 10 - 4059

Hon.

ECF Case

TRAGER, J.
AZRACK, M.J.

COMPLAINT

NATURE OF THE ACTION

1. This is a constitutional challenge to Department of Homeland Security (DHS) policies that authorize the suspicionless search of the contents of Americans' laptops, cell phones, cameras and other electronic devices at the international border. Between October 1, 2008 and June 2, 2010, over 6,500 people – nearly 3,000 of them U.S. citizens – were subjected to a search of their electronic devices as they crossed U.S. borders. The challenged policies were issued by DHS components U.S. Customs and Border Protection (CBP) and U.S. Immigration and Customs Enforcement (ICE). The policies apply to all electronic devices that "contain

information," including laptops, cameras, mobile phones, "smart" phones, and data storage devices. The policies permit border agents to search and copy electronic devices without reasonable suspicion. The policies also allow border agents to detain electronic devices and continue their searches even after a traveler has been permitted to enter the country. The policies do not place any time limits on how long DHS can keep travelers' devices, nor do they limit the scope of private information that may be searched, copied, or detained. The policies contain no meaningful limits on what information gleaned from a search can be retained and with whom that information can be shared. The policies make no provision for judicial approval or supervision.

2. Plaintiffs in this case are a U.S. citizen who has had his laptop, external hard drive, and cell phones searched and detained at the border and two U.S. professional associations whose members have had their electronic devices searched in the past. Both the individual plaintiff and the associations' members are likely to have their electronic devices searched, copied, and/or detained in the future pursuant to the policies. All have expended time, effort, and in some cases money to mitigate the harm that will be caused by such searches in the future.

3. Electronic devices like laptops, "smart" phones, and external data storage devices hold vast amounts of personal and sensitive information that reveals a vivid picture of travelers' personal and professional lives, including their intimate thoughts, private communications, expressive choices, and privileged or confidential work product. CBP's and ICE's policies and practices of searching, copying, and detaining these personal devices without suspicion or judicial supervision violates the constitutional rights of American citizens to keep the private and expressive details of their lives, as well as sensitive information obtained or created in the course of their work, free from unwarranted government scrutiny. The plaintiffs seek declaratory relief,

an injunction against further enforcement of the policies, and the return or expungement of materials unlawfully obtained from Mr. Abidor's laptop.

JURISDICTION AND VENUE

4. This case arises under the Constitution of the United States and presents a federal question within this Court's jurisdiction under 28 U.S.C. § 1331.

5. The Court has authority to issue declaratory and injunctive relief under 28 U.S.C. §§ 2201 and 2202, Rules 57 and 65 of the Federal Rules of Civil Procedure, and its inherent equitable powers.

6. Venue is proper in this district under 28 U.S.C. § 1391(e)(3) because plaintiff Pascal Abidor resides in this district.

PARTIES

7. Plaintiff Pascal Abidor is a twenty-six-year-old U.S.-French dual citizen and a Ph.D. student at the Institute of Islamic Studies at McGill University in Montreal, Canada. Mr. Abidor is a resident of Brooklyn, New York, where his family lives.

8. Plaintiff the National Association of Criminal Defense Lawyers ("NACDL") is a 501(c)(6) non-profit organization based in Washington, D.C. NACDL is the association of the nation's criminal defense bar and has members in every state, including New York. NACDL sues on behalf of its members.

9. Plaintiff the National Press Photographers Association ("NPPA") is a 501(c)(6) non-profit organization based in North Carolina and incorporated in New York whose membership is comprised of approximately 7,000 professional and freelance photojournalists. NPPA has members in every state as well as more than 250 members who reside abroad. More than 500 NPPA members reside in New York State. NPPA sues on behalf of its members.

10. Defendant Janet Napolitano is the Secretary of the Department of Homeland Security. CBP and ICE are components of DHS. As head of DHS, Secretary Napolitano has authority over all DHS policies, procedures, and practices related to border searches, including those challenged in this lawsuit. Defendant Napolitano is sued in her official capacity.

11. Defendant Alan Bersin is Commissioner of CBP. Commissioner Bersin has authority over all CBP policies, procedures, and practices relating to border searches, including those challenged in this lawsuit. Defendant Bersin is sued in his official capacity.

12. Defendant John T. Morton is Assistant Secretary of Homeland Security for ICE. Assistant Secretary Morton has authority over all ICE policies, procedures, and practices relating to border searches, including those challenged in this lawsuit. Defendant Morton is sued in his official capacity.

FACTUAL ALLEGATIONS

The Policies

13. In August 2009, two components of DHS issued substantially similar policies regarding the search, copying, and detention of electronic devices at the border: CBP issued a policy entitled "Border Search of Electronic Devices Containing Information" (the "CBP Policy"), CBP Directive No. 3340-049 (Aug. 20, 2009), and ICE issued a policy entitled "Border Searches of Electronic Devices" (the "ICE Policy"), ICE Directive No. 7-6.1 (Aug. 18, 2009). Both policies define "electronic devices" as any devices that "contain information," such as computers, disks, drives, tapes, mobile phones, cameras, and music players.

14. Both policies permit border officials to read and analyze the contents of information on international travelers' electronic devices without any suspicion of wrongdoing. The CBP Policy states that, in the course of a border search, "with or without individualized suspicion, [a

CBP officer] may examine electronic devices and may review and analyze the information encountered at the border." The ICE Policy states that, "ICE Special Agents acting under border search authority may search, detain, seize, retain, and share electronic devices, or information contained therein, with or without individualized suspicion." Under both policies, these searches may occur outside of the traveler's presence.

15. Both policies permit border officials to read and analyze – without individualized suspicion – even legal or privileged information, information carried by journalists, medical information, confidential business information, and other sensitive data. The only limitations on such searches are that CBP or ICE agents must, in some circumstances, first consult with supervisors, agency counsel, or the U.S. Attorney's Office, and that the searches must comply with any other applicable federal law or policy.

16. Both policies permit border officials, without any suspicion of wrongdoing, to detain a traveler's electronic devices, or copies of the contents thereof, for the purpose of further reading and analysis even after the traveler has left the border. These detentions and searches may take place either on- or off-site. Although varying levels of supervisory approval are required for lengthy detentions, there is no specified maximum amount of time that a detention or search may continue.

17. When agents need technical advice to conduct a search, the policies permit border agents to share a traveler's devices or copies of the contents of those devices with other government agencies or third parties even where there is no suspicion of wrongdoing. When agents need "subject matter assistance" to conduct a search, the policies permit them to share a traveler's devices or copies of the contents of those devices with other government agencies or third parties when they have reasonable suspicion of activities in violation of the laws that CBP

and ICE enforce. If CBP or ICE transmits a device or copy to another federal agency for assistance, the assisting federal agency may retain or seize the device or copy when it has independent legal authority to do so.

18. In certain circumstances, the policies permit border agents to permanently retain copies of the contents of a traveler's electronic devices or information derived from the devices without any suspicion of wrongdoing. For example, both CBP and ICE may retain information without probable cause when it is "relevant" to immigration, customs, and other enforcement matters, and "if such retention is consistent with the privacy and data protection standards of the [pertinent records] system."

19. When agents have decided to permanently retain information from a traveler's electronic devices, the policies permit border officials to share that information "with federal, state, local and foreign law enforcement agencies."

20. According to records released by CBP through the Freedom of Information Act, between October 1, 2008 and June 2, 2010, over 6,500 people were subjected to a search of their electronic devices as they crossed U.S. borders. Of these, nearly 3000 were U.S. citizens. Between October 28, 2008 and June 9, 2009, CBP detained over 220 electronic devices carried by international travelers. Between July 2008 and June 2009, CBP transferred data its agents found on travelers' electronic devices to third party agencies over 280 times. Over half the time, those third party agencies asserted an independent basis for retaining or seizing the data.

PLAINTIFFS' ALLEGATIONS

Pascal Abidor

21. Pascal Abidor is a twenty-six year old U.S.-French dual citizen and a graduate student in Islamic Studies at McGill University in Montreal, Canada. Mr. Abidor stores a large amount of personal and private information on his laptop and other electronic devices. For example, his laptop and external hard drive contain everything from his academic research and reading materials, class notes, emails and chat records with his girlfriend and friends, photos of friends and family, his favorite movies and music, journal articles of interest, documents detailing his academic credentials, tax records, and images downloaded from the Internet. A quick search of his laptop reveals what files he has recently downloaded from the Internet, what Web sites he has recently visited, and what search terms he has entered into search engines such as Google.

22. Mr. Abidor frequently travels internationally with his electronic devices. As a Ph.D. student in Islamic Studies, Mr. Abidor travels abroad to pursue his research. He brings his laptop and other devices with him when he travels so he can access necessary research materials and record the results of his archival and other research. Furthermore, as a U.S. citizen attending school in Canada, Mr. Abidor regularly crosses the border on trips home to Brooklyn. He brings his laptop and other devices with him when he returns home because these devices are his virtual office, allowing him to access his personal correspondence and other documents at all times.

23. Mr. Abidor treats the contents of his electronic devices as private and has always believed they are private. Much of the information stored in Mr. Abidor's laptop and other electronic devices is highly personal, and reveals intimate details about Mr. Abidor's life, including his thoughts, his associations, his scholarly work, and his expressive choices. Mr.

Abidor ensures that his laptop remains protected by locking it with a password and using security software.

May 1 Search of Mr. Abidor's Laptop

24. On Saturday, May 1, 2010, at about 9 a.m., Mr. Abidor boarded Amtrak train 69 in Montreal, Canada, with the final destination of New York City, to visit his family after the end of the academic year at McGill University. He was carrying his laptop, digital camera, two cell phones, and external hard drive.

25. At approximately 11 a.m., the train arrived at the CBP inspection point at the border of Québec and New York, in the vicinity of Service Port-Champlain.

26. At the inspection point, a CBP officer named Officer Tulip boarded the train and approached Mr. Abidor. Mr. Abidor gave her his customs declaration and U.S. passport.

27. Officer Tulip asked where Mr. Abidor lives and why. Mr. Abidor explained that he lives in Canada because he is pursuing a graduate degree in Islamic Studies.

28. Officer Tulip then asked him where he had been the previous year. Mr. Abidor told her that he had briefly lived in Jordan and been to Lebanon. He provided her with his French passport, which contained the visas to those two countries.

29. After this brief interaction, Officer Tulip directed Mr. Abidor to bring his belongings to the café car of the train for further inspection. Upon seeing Mr. Abidor's belongings, Officer Tulip took and carried the bag containing Mr. Abidor's laptop as she escorted him to the café car.

30. There were five or six other CBP officers present in the café car. When Officer Tulip and Mr. Abidor entered the café car, Officer Tulip, without any further questioning or warning,

removed Mr. Abidor's laptop from his bag and turned it on. She ordered Mr. Abidor to enter his password. Mr. Abidor complied with the order.

31. Once Officer Tulip gained access to the laptop, she began to peruse its contents.

32. While browsing through his laptop, Officer Tulip asked Mr. Abidor about some personal pictures she found as well as pictures that Mr. Abidor had downloaded from the Internet for research purposes. The images that Mr. Abidor had downloaded from the Internet for research purposes, including images of Hamas and Hezbollah rallies, particularly interested Officer Tulip. She asked Mr. Abidor why he had "this stuff" on his computer. Mr. Abidor explained that he had gotten the images through a Google Image search. She asked why he would be interested in the images, and Mr. Abidor explained that his specific area of research for his Ph.D. degree is the modern history of Shiites in Lebanon.

33. At this point, Officer Tulip and other CBP officers ordered Mr. Abidor to write down his password. Mr. Abidor complied with this order. The officers asked him a few other questions on topics such as his girlfriend, the purpose of his studies, where he had lived since 2006, and his plans during the next few years.

34. The officers then told Mr. Abidor that he would be taken off the train to the port. A male officer directed him to put his hands against the wall of the café car. He patted Mr. Abidor down, applying a strong amount of pressure to his groin and genitals at various angles. The officers then placed Mr. Abidor in handcuffs. The officers told him that frisking and handcuffing was standard procedure.

35. Mr. Abidor arrived at the port at approximately 1 p.m. A number of agents carried Mr. Abidor's belongings into the building. Mr. Abidor was placed in a detention cell without any of his luggage. The cell, which was approximately 5 feet by 10 feet, had painted

cinderblock or concrete walls, and there was a concrete and steel-reinforced door with a small window.

36. Mr. Abidor was detained for approximately three hours. During that time, he was questioned by Officer Tulip and several other officers. Occasionally someone would enter the cell and ask a few questions. When Mr. Abidor was questioned at length, the officers took him outside of the cell.

37. During the questioning, the agents told Mr. Abidor that he had lots of "symbolic materials" in his possession and that he needed to explain the meaning of the materials and why he possessed them. They also asked him about his parents, travel history and plans, Ph.D. research topic, and his perspective on the Middle East.

38. After Mr. Abidor answered their questions, truthfully and to the best of his ability, the officers took Mr. Aibdor to a separate room to take his fingerprints and photograph him. He was then returned to the detention cell.

39. An officer who described himself as working both with CBP and with the FBI subsequently entered the detention cell to ask Mr. Abidor more questions. The officer asked him about his Ph.D. research topic, his interest in the topic, and future plans. Once again, Mr. Abidor answered all questions truthfully and to the best of his ability.

40. Sometime after Mr. Abidor spoke to the officer from CBP and FBI, Officer Tulip came to his detention cell and told him that he would be free to go in five minutes once the paperwork was completed.

41. On information and belief, during the three hours in which Mr. Abidor was being questioned, officers from CBP and/or other government agencies searched through various files on his laptop. For example, from what Mr. Abidor could determine from the "last opened" date

of the files after his laptop was returned, during that three-hour period, the officers at minimum opened an iMovie Project entitled "My Great Movie" and an Adobe PDF document of citations for his dissertation.

42. As Mr. Abidor was being released, he learned that CBP would not return his laptop and external hard drive to him. He insisted that he needed access to these devices for research purposes and that he would be traveling to the United Kingdom and France to do research in two weeks. He was particularly concerned because the devices contained the sole copies of his academic work product from the past three years.

43. Officer Tulip gave Mr. Abidor a "Detention Notice and Custody Receipt for Detained Property." The form indicated that the devices were being held for ICE.

44. Mr. Abidor received his other luggage, including his camera and two cell phones. One of his cell phones was returned with a scratch on the back of the phone near the battery, suggesting that someone had tried to open it.

45. Mr. Abidor was released at approximately 4 p.m., almost five hours after his train arrived at the U.S.-Canada crossing. Because he had been taken off his train, he had to wait for a bus with an open seat to take him into New York City. He finally arrived at his home in New York City at around midnight.

46. The encounter with CBP and FBI agents left Mr. Abidor frightened, disturbed and severely upset. For at least 10 days, Mr. Abidor had a difficult time sleeping. He was in a state of anxiety and experienced panic attacks.

Eleven-Day Detention of Mr. Abidor's Laptop and External Hard Drive

47. In the days following his return to the United States, Mr. Abidor repeatedly called the seized property office at Service Port-Champlain to ask when his laptop and external hard drive

would be returned. He was anxious to have the devices returned to him because they contained the sole copies of his academic work and because he was planning to leave for Europe in two weeks for archival work. He was told only that the government claims the authority to keep the devices for up to 30 days.

48. On May 10, 2010, CBP received a letter from Mr. Abidor's lawyers demanding the immediate return of his electronic devices. On May 12, 2010, Mr. Abidor finally received the laptop and external hard drive via mail.

49. Mr. Abidor's laptop has a seam between the keyboard portion of the laptop and the outer case, which would reveal the internal hard drive if opened. Upon return, there appeared to be minor increases of space in the seam of the laptop. The external hard drive was returned with the casing and warranty seal broken open.

50. By examining the "last opened" date of files on his laptop, Mr. Abidor learned that between May 1 and May 11, officers from ICE, CBP and/or other agencies had examined basic directory folders on his laptop such as "library" and "users," as well as backup documents that he had stored on his external hard drive.

51. Some files opened and examined by the officers included highly private and expressive materials that reveal intimate details about Mr. Abidor's life, such as his personal photos, a transcript of a chat with his girlfriend, copies of email correspondence, class notes, journal articles, his tax returns, his graduate school transcript, and his resume. At the time his laptop was detained, it was configured to automatically allow access to his online email and social networking accounts, raising the possibility that border agents searched through Mr. Abidor's stored correspondence and communications as well.

52. On information and belief, officers from ICE, CBP and/or other agencies copied the contents of Mr. Abidor's laptop and external hard drive.

53. On information and belief, officers from ICE, CBP and/or other agencies transmitted the contents of Mr. Abidor's laptop and external hard drive to other agencies.

54. On information and belief, copies of the contents of Mr. Abidor's laptop and information derived from his devices are being retained by ICE, CBP and/or other agencies.

Future Travels Across the U.S. Border

55. Mr. Abidor's electronic devices are likely to be searched and detained in the future pursuant to ICE's and CBP's suspicionless search policies. As a graduate student, Mr. Abidor travels frequently across the U.S. border with his electronic devices. He often travels with a number of such devices, including his laptop, external hard drive, cell phone, camera, and iPod. When he travels to attend school in Canada, and also when he travels to countries in Europe and the Middle East to conduct research, Mr. Abidor is often out of the country for weeks or months at a time.

56. Mr. Abidor is likely to be subjected to search under ICE's and CBP's suspicionless search policies because Officer Tulip appeared to decide to search his laptop on the basis of two factors that will not change – his field of study and his past travels.

57. Mr. Abidor has just started his graduate program at McGill University in Montreal, Canada, and plans to be there for at least five more years. In the past year since he started his program, he has returned to the United States twice to visit his family in New York. He plans to continue returning home for a visit at least two to three times each year.

58. Mr. Abidor also plans to travel to and from the United States to countries in Europe and the Middle East to conduct research for his degree. For example, on May 16, 2010, Mr.

Abidor flew from John F. Kennedy International Airport to the United Kingdom and France in part to do archival work. He returned to the United States through Newark Liberty International Airport on July 8, 2010. Upon his return, he was referred to secondary inspection. His electronic devices were not searched, but it became apparent that information about his previous encounter with officials at Service Port Champlain, and possibly information derived from the searches of his electronic devices, was accessible to the CBP officer at Newark. Mr. Abidor was questioned about what happened to him the last time he was stopped, what he intended to do once he received his Ph.D., how he paid for his travels, and details about his girlfriend. He was also asked whether he was a Muslim, and what languages he speaks.

59. As his research progresses, Mr. Abidor expects to travel more frequently. For example, he will have to travel to Syria and Lebanon to complete his Ph.D. thesis. When Mr. Abidor travels internationally to conduct research, he must travel with his laptop to transport research materials and record the results of his research.

60. As a result of CBP's and ICE's suspicionless search policies, Mr. Abidor must take steps to safeguard his private, expressive, and research material from unwarranted government scrutiny at the border and take steps to minimize the risk that border officials will once again seize his electronic devices for a lengthy period of time.

61. It is not feasible for Mr. Abidor to leave his electronic devices behind when he travels internationally. Mr. Abidor needs these devices with him so he can transport research materials, record the results of his research, and communicate with others.

62. Mr. Abidor has already started traveling with less information on his computer. Given his area of study, Mr. Abidor is particularly concerned about having information on his laptop that could be misconstrued by border officials. He now self-censors what types of

photographs he downloads to his computer. Even for those materials that he does download, prior to traveling, Mr. Abidor now backs up onto an external hard drive and then deletes materials he fears that border officials may misconstrue, and that may lead border officials to detain him and his electronic devices. Mr. Abidor no longer stores the passwords for his email and social networking accounts on his computer.

63. Mr. Abidor has also decided to change the way he conducts research. When he conducts archival research, Mr. Abidor now avoids taking notes and gathering materials of the type that might by misconstrued by border officials. Also, he will now, where possible, forego taking notes of his interviews with research subjects. When Mr. Abidor does take notes of interviews with research subjects or when interview subjects provide him with documents and information, he will warn them of the possibility that border officials will obtain access to this information under the suspicionless search policies. Mr. Abidor fears that this will discourage some interviewees from being candid or from sharing information or documents with him that they otherwise would have shared.

64. Mr. Abidor has also changed the manner in which he travels to visit his family. Before the incident at Service Port Champlain, Mr. Abidor typically traveled home from McGill University via Amtrak because it is substantially cheaper than flying and is faster (and often cheaper) than renting a car in Montreal and returning it in New York. Now, he intends to rent a car to travel between school and his home. Although border officials may still search his devices and detain him, traveling by car will be less disruptive to his travel plans than being taken off an Amtrak train, transported to the far-away Service Port Champlain, and then waiting for a bus to take him home once he is permitted to leave the port. When Mr. Abidor returned to

school on August 6, he rented a car to drive across the border to avoid the possibility of being stranded at the port.

National Association of Criminal Defense Lawyers

65. The National Association of Criminal Defense Lawyers ("NACDL") is a non-profit organization founded in 1958 to promote study and research in the field of criminal law; to disseminate and advance knowledge of the law in the area of criminal practice; and to encourage the integrity, independence, and expertise of defense lawyers in criminal cases.

66. NACDL is a membership organization with approximately 10,000 lawyers and 35,000 affiliate members from all 50 states, six U.S. territories, and 32 nations.

67. NACDL actively advocates to protect the constitutional rights of its members and its members' clients. NACDL is concerned with the erosion of due process and the rights of criminal defendants and suspects generally, but is particularly concerned with the impact that national security policies implemented in the past 10 years have had on the criminal justice system and the way in which they have eroded First, Fourth, Fifth, and Sixth Amendment rights.

68. NACDL has been particularly active in protecting its members and their clients against unconstitutional government surveillance policies and practices. To this end, among other things, NACDL has lobbied against or for the repeal of unconstitutional surveillance laws and policies such as provisions of the Patriot Act, the National Security Agency's (NSA) warrantless wiretapping program, and the FISA Amendments Act. NACDL has sued on behalf of its members to challenge the legality and constitutionality of the NSA's warrantless wiretapping program. NACDL has also submitted *amicus curiae* briefs in cases concerning border searches and government surveillance. *See, e.g.*, Brief *Amicus Curiae* of the National Association of Criminal Defense Lawyers in Support of Respondent, *United States v. Flores-*

Montano, No. 02-1794 (Jan. 12, 2004) (concerning constitutionality of a suspicionless border search); Brief on Behalf of *Amicus Curiae* National Association of Criminal Defense Lawyers in Support of Affirmance, *In Re Appeal from July 19, 2002 Decision of the United States Foreign Intelligence Surveillance Court*, No. 02-001 (For. Intel. Surv. Ct. of Rev. Sept. 9, 2002) (brief concerning constitutionality of Patriot Act amendments to Foreign Intelligence Surveillance Act); Brief on Behalf of the National Association of Criminal Defense Lawyers *et al.* as *Amici Curiae*, *People v. Weaver*, No. 53 (N.Y. Feb. 2, 2009) (concerning constitutionality of warrantless GPS tracking of personal vehicle).

69. Because of the nature of their work, many NACDL members routinely travel abroad for professional purposes and bring their electronic devices with them. Many NACDL members routinely travel abroad because they are employed by large U.S.-based law firms that maintain offices in multiple foreign countries and must travel abroad to collaborate on cases with their foreign colleagues.

70. Many NACDL members regularly travel abroad as part of their representation of their clients, either because they represent clients who live abroad, or because they must travel abroad to gather evidence or engage in other activities related to their clients' cases. For example, at least fifty NACDL members currently represent or have represented terrorism suspects who are either foreign nationals or who have allegedly engaged in illegal terrorist activity abroad. In the course of representing these clients, members travel internationally to meet with witnesses, foreign counsel, experts, journalists, and government officials.

71. Similarly, many NACDL members defend, and some are currently defending, death penalty cases that necessitate overseas investigations. In all capital cases, the American Bar Association's "Guidelines for the Appointment and Performance of Defense Counsel in Death

Penalty Cases" demand that defense lawyers seek information that "supports mitigation or rebuts the prosecution's case in aggravation." There is no exception. Where such information resides abroad, members have a professional obligation to conduct an international mitigation investigation.

72. International travel for evidence-gathering purposes is also often unavoidable for the many NACDL members who represent clients fighting extradition to or from the United States or who defend clients charged under the Foreign Corrupt Practices Act – cases that typically involve companies, individuals, and evidence outside of the United States. NACDL members are involved in both types of cases.

73. International travel is even more frequent now for NACDL members as a result of recent changes to electronic surveillance law. The 2008 FISA Amendments Act made it much easier for the government to intercept the international communications of criminal defense lawyers representing overseas clients or conducting investigations abroad. As a consequence, many attorneys are ethically obligated to safeguard client confidences by meeting face-to-face with clients and witnesses located abroad, which in turn necessitates much more international travel.

74. Some NACDL members also frequently travel abroad to attend professional seminars and conferences, including conferences hosted by NACDL itself. For example, this year's NACDL annual meeting took place in Toronto, Canada. As a result, 68% of the NACDL members in attendance had to travel to Canada from the United States.

75. When NACDL members travel for work-related purposes, they almost invariably travel with electronic devices such as laptop computers, flash drives and other electronic storage devices, cell phones, and digital recording devices. Such equipment is necessary to take notes,

record interviews, perform legal research, draft legal documents, and communicate with clients, witnesses, law firm staff, investigators, and/or co-counsel. NACDL members also frequently need access to the case files and other documents that their electronic devices contain. In today's world, portable computing devices and electronic communications equipment comprise a "virtual law office," allowing a diligent attorney to work virtually anywhere at any time.

76. In addition to their professional materials, NACDL members' electronic devices also often contain vast amounts of personal, private, and expressive data, such as their own personal financial records, family photographs, and communications with friends and family.

77. The ICE and CBP suspicionless search policies harm NACDL's members by interfering with their ability to do their work. Because the ICE and CBP policies are not limited to authorizing searches of those suspected of any wrongdoing, NACDL members must take seriously the risk that the content of their electronic devices could be reviewed, copied, and detained.

78. NACDL members have an ethical duty to safeguard the confidentiality of their clients' information, as well as other privileged and work product information. The attorney-client privilege is part of the very foundation on which the adversarial system was built and embodies the bedrock principle that the public interest is best served when lawyers are able to counsel their clients based on a candid understanding of the relevant facts. The privilege is essential to the effective assistance of counsel because it helps foster the trust necessary to encourage full and frank discussion with counsel. The attorney-client privilege makes it possible for an attorney to obtain the facts necessary to mount an informed defense and advise clients on compliance with the law.

79. The ICE and CBP search policies permit NACDL members' confidential work product or attorney-client privileged materials to be searched at will by agents of the same federal government that seeks to prosecute, imprison, or execute their clients. The damage inflicted by such a search would be devastating to the attorney-client relationship as well as the clients' Fifth and Sixth Amendment rights. The suspicionless search policies therefore create a serious ethical dilemma for defense attorneys who determine that competent representation requires international travel but recognize their ethical obligation to avoid situations that might inadvertently disclose client confidences. The failure to exercise reasonable care in protecting client confidences can be cause for disciplinary action by some state bars and may constitute malpractice in some states. This problem is particularly acute where disclosure to a litigation adversary – typically the federal government – is likely.

80. It is infeasible for attorneys to travel overseas without their electronic devices. In today's digital world, there is no practical alternative to working with electronic data and files. Essentially all legal work product is now digital. This includes court documents such as opinions, orders and filed pleadings; legal authorities accessible through services such as Westlaw and Lexis; correspondence with clients, opposing counsel, and witnesses; discovery materials; and attorney notes of meetings with clients and others. It is difficult if not impossible for attorneys working abroad to function effectively without bringing their laptops and other electronic devices with them.

81. When exiting the country, lawyers must either take the electronic devices they normally use in the course of business with them, or must travel with separate devices that have no or at least less sensitive or privileged information on them. If they take their usual devices with them, they will cross the border with a great deal of privileged and sensitive information,

not just about the case for which they are traveling but also about other client matters and possibly also their own personal records. Yet taking a separate travel device is burdensome, not only entailing the time and expense of purchasing duplicate electronic devices, but also the costs associated with deleting all information on the device, where even feasible, for every trip and uploading it with whatever information is necessary for the new trip.

82. Moreover, attorneys who travel for work purposes generate privileged or confidential information while abroad. When attorneys carry this information back to the United States on their electronic devices, they run the risk that it will be subjected to a search by border agents.

83. Because defense attorneys have an ethical obligation to avoid situations that might inadvertently disclose client confidences, the search policy requires some NACDL members to refrain from taking notes or making recordings of certain meetings while abroad. NACDL members subjected to a government search of their confidential or privileged files face a dramatically increased risk of losing the client confidence necessary to foster full and open discussions about the facts and legal strategy of their cases.

84. Because many NACDL members routinely travel abroad with a wide range of electronic devices, many of which will invariably contain sensitive and privileged information, NACDL fears that its members' electronic devices will be searched, copied, and detained by U.S. border officials under the ICE and CBP policies.

85. At least one NACDL member has already been subject to a suspicionless search of her laptop.

86. Lisa M. Wayne is a criminal defense attorney in private practice based in Denver, Colorado. She currently serves as NACDL's President-Elect. Ms. Wayne handles serious felonies and complex civil litigation including numerous high profile cases. Ms. Wayne is an

adjunct law professor at the University of Colorado, where she teaches Trial Advocacy. She also serves on the faculty of the Trial Practice Institute at Harvard Law School, the National Criminal Defense College (NCDC), and Cardozo Law School. She lectures nationally with NACDL, the National Institute of Trial Advocacy (NITA), the American Bar Association, and various other organizations. She is also a legal analyst for CNN. In 2005, Ms. Wayne was honored with the Robert J. Heeney Award, NACDL's most prestigious recognition. Earlier in her career, Ms. Wayne was a Colorado State Public Defender for 13 years.

87. Ms. Wayne frequently travels to Mexico in connection with the Mexico Legal Reform Project, a partnership between NITA, Southwestern Law School, Tecnológico de Monterrey, Texas Tech University School of Law, and the ABA Section on International Law. The project is funded by a United States Agency for International Development's (USAID) grant to provide oral advocacy training to Mexican attorneys. Ms. Wayne often travels as an observer and advisor to the program.

88. Ms. Wayne frequently travels abroad with electronic devices, including a laptop computer, cell phone, and electronic storage devices. When traveling, Ms. Wayne's laptop is her "traveling office." She uses it to store and transport client files, take notes of meetings and interviews, and draft legal memoranda about those meetings and interviews. She maintains contact with her physical office in the United States via cell phone and email, which may be sent and received on her laptop or cell phone. Many of these communications are likely to be privileged or confidential and may concern cases unrelated to the purpose of travel.

89. In August, 2008, Ms. Wayne traveled to Oaxaca, Mexico, for one of NITA's trial advocacy programs. Ms. Wayne functioned as an observer.

90. Following the NITA program, Ms. Wayne boarded a Continental Airways flight from Oaxaca to George Bush Intercontinental Airport (IAH) in Houston, Texas, with a scheduled connecting flight to Denver, Colorado.

91. Upon arrival at IAH, Ms. Wayne cleared passport control, claimed her checked baggage, and entered the CBP inspection area in Terminal E.

92. After retrieving her baggage in the inspection area, Ms. Wayne was selected for a secondary search of her belongings. She was escorted to a separate room in the inspection area where a CBP officer sat at a desktop computer with a screen that was not visible to Ms. Wayne. Ms. Wayne surmised that the officer was looking at a file containing information about Ms. Wayne when he remarked, "I see you're a defense lawyer." The officer then asked who she was seeing in Mexico. Ms. Wayne responded that she wouldn't be a very good attorney if she revealed to the agent who she had been seeing. Ms. Wayne inquired whether she was on a "list" and had been selected for additional screening for that reason. The officer told Ms. Wayne that she was not on a "list" but could not tell her the source or substance of the information he had about her.

93. The CBP officer then conducted a search of Ms. Wayne's luggage, including her clothing and lingerie. Following this physical search, the CBP officer directed Ms. Wayne to power on her laptop computer and enter in her password.

94. Ms. Wayne was unaware of the search policy and did not realize that the CBP officer planned to examine the contents of her laptop. Ms. Wayne is accustomed to having her laptop inspected every time she enters a courthouse and passes through the security checkpoint, often multiple times a week. Similarly, she is accustomed to entering her login password at the request of courthouse security officials attempting to determine whether her laptop functions

normally. Courthouse security officials have never sought to examine the contents of Ms. Wayne's computer, even after asking Ms. Wayne to enter her password. Ms. Wayne mistakenly believed the CBP officer would follow a similar procedure. She did not anticipate that the officer would search the contents of her laptop.

95. The CBP officer took Ms. Wayne's computer out of sight for more than 30 minutes, presumably to complete an electronic search. Ms. Wayne did not witness the CBP officer's search. After the officer returned with Ms. Wayne's laptop, he granted Ms. Wayne reentry into the United States. She was detained for a total of approximately 45 minutes, causing her to miss her connecting flight home to Denver. Ms. Wayne remains outraged at the indignity and invasiveness of having a CBP officer search the contents of her laptop computer for no apparent reason.

96. As a frequent international traveler, Ms. Wayne will encounter CBP agents every time she crosses the border. Ms. Wayne has concrete plans for future international travel. Ms. Wayne is planning to travel to Mexico and El Salvador in the upcoming months related to both NITA training as well as client investigation on a pending case. She plans to bring her cell phone and laptop computer on these trips in order to contact witnesses and other individuals relevant to her investigation as well as to take detailed notes of her meetings. During the course of this international investigation, Ms. Wayne also plans to generate memoranda of her meetings, interviews of witnesses, and other information. The notes and memoranda Ms. Wayne generates on her laptop will constitute confidential attorney work product and are likely to contain privileged information. Her laptop will also contain privileged and confidential documents from unrelated cases.

97. Ms. Wayne plans to protect these privileged and confidential documents from a border search by refusing to divulge the password required to view these files and asserting the attorney-client privilege. Ms. Wayne fears that CBP agents may nonetheless detain her laptop and ultimately gain unauthorized access to its contents with the "technical assistance" of agents capable of overriding her password.

98. Because of ICE's and CBP's laptop search policies and because of the prior search of her laptop, Ms. Wayne fears that her electronic devices – and the privileged information therein – will once again be searched, copied and/or detained by U.S. government officials pursuant to the policies.

National Press Photographers Association

99. Plaintiff the National Press Photographers Association ("NPPA") is dedicated to the advancement of visual journalism, its creation, practice, training, editing, and distribution in all news media, and works to promote visual journalism's role as a vital public service. Visual reporting is a uniquely powerful way to communicate because images can convey information and narratives in compelling ways that transcend language and cultural barriers.

100. NPPA's approximately 7,000 members are professional and freelance photojournalists. NPPA's diverse membership includes television and still photographers, editors, students and others who work or freelance in photography, multimedia, audio, video, design, editing, producing, teaching, writing, reporting, or visual journalism on the Web. NPPA has members in every state as well as more than 250 members who reside abroad. More than 500 NPPA members reside in New York State.

101. Since 1946 the NPPA has vigorously promoted freedom of the press in all its forms, especially as that freedom relates to photojournalism. NPPA works to ensure robust protection

of photojournalists' constitutional rights to gather and publish news and news images, to speak freely, and to be free from unwarranted government surveillance. NPAA actively advocates against laws and government policies that restrict or chill their members' ability to freely gather news and to publish and disseminate images and information to the world. To this end, NPPA, among other things, has sued on behalf of its members to challenge a federal law that prohibited publication of "indecent" material on the Internet. *See ACLU v. Reno*, 521 U.S. 844 (1997). NPPA has also submitted *amicus curiae* briefs in numerous cases of constitutional significance to journalists and photojournalists. *See* Brief of *Amici Curiae* National Press Photographers Association *et al.* in Support of Plaintiff-Appellant, *Courtroom Television Network LLC v. State of New York*, No. 88 (N.Y. Jun 16, 2005) (concerning cameras in the courtroom); Brief for The Reporters Committee for Freedom of the Press, *et al.* as *Amici Curiae* in Support of Respondents, *Snyder v. Phelps*, No. 09-751 (U.S. appeal docketed Mar. 8, 2010) (concerning journalists' ability to report on, photograph, and film video footage near military funerals); Brief for ABC, Inc. *et al.* as *Amici Curiae* Supporting Respondents-Appellants, *Chevron v. Berlinger*, No. 10-1918 (2nd Cir. docketed May 19, 2010) (concerning application of reporters privilege to photojournalists' outtake material); Brief for The Reporters Committee for Freedom of the Press, *et al.* as *Amici Curiae* Supporting Petitioner, *Hammer v. Ashcroft*, No. 09-504 (U.S. Mar. 8, 2010) (concerning death row inmate's right to speak to the press), *cert. denied*, 130 S. Ct. 1735 (2010).

102. Because of the nature of their work, many NPPA members routinely travel abroad for professional purposes. Some NPPA members must often travel abroad to cover global news stories, including wars and violent conflicts, political unrest, large-scale protests, natural disasters, international summits and conferences, elections and political developments in foreign

countries, and global sporting events. Other NPPA members must often travel abroad for professional purposes because they specialize in travel news and photography.

103. NPPA members often cover news stories that are of interest to the United States government. For example, NPPA members frequently cover stories relating to political developments in foreign countries, violent conflicts, civil unrest, and international crime. In the course of covering these stories, NPPA members often come into contact with and document individuals who may be of interest to the U.S. government.

104. NPPA members who cover international stories must, by definition, capture and document first-hand images, video, and audio. They must also capture images and footage of interview subjects and sources.

105. When covering stories abroad, NPPA's members do more than just take pictures and videotape. NPPA members also develop the content of stories by conducting interviews and gathering information from sources. They also write news articles or text to accompany the images they document, and create videos and make video and multimedia news pieces.

106. In addition to their own independent reporting, NPAA members also often accompany traditional print and broadcast journalists to take photographs or video footage of other journalists' interview subjects and sources. For example, NPPA member Scott McKiernan, CEO of ZUMA Press, Inc. travels abroad with his gear 45-60 days a year, visiting approximately 12 countries. NPPA member Rick Loomis travels overseas 5-6 times a year on assignment as a staff photographer for the Los Angeles Times. During the past 18 months he has been in India, the UAE, Afghanistan, Haiti, Morocco, China, Kenya, South Africa, Uganda and the Philippines.

107. When NPPA members travel for work or assignments abroad, they travel with electronic devices that are necessary for them to carry out their work. These devices include

cameras, laptops, media storage devices, hard drives, cell phones, iPhones and Blackberries. They use these devices while abroad to capture and store imagery; make and store videos; take and store notes; write and transmit stories; and communicate with sources, reporters, and the newsrooms or media outlets for which they are working.

108. The days of film and the darkroom are long gone. News images are no longer processed and printed in a lab or darkroom. Now, news images must be uploaded to a computer. Video and multimedia news pieces must be created on a computer, often a laptop. The same is true of interview notes and other text created to accompany a photojournalist's images. NPPA members must also store the images, video, text, and notes they gather in the course of covering a story on a laptop, flash drive, hard drive, or other media storage device. NPPA members must also use their electronic devices to communicate with sources, reporters, and the newsrooms or media outlets for which they are working.

109. In addition to their work product, NPPA members' electronic devices also often contain vast amounts of personal, private, and expressive data. NPPA members often travel for weeks or even months at a time. Their electronic devices allow them to maintain their personal financial, medical and other records and communicate with friends and family in the United States and around the world.

110. The ICE and CBP suspicionless search policies harm NPPA's members by interfering with their ability to do their work. Because the ICE and CBP policies are not limited to authorizing searches of those suspected of any wrongdoing, NPPA members must take seriously the risk that the content of their electronic devices could be read, viewed, or listened to or copied by border agents.

111. The ability to keep work files related to potential news stories free from unwarranted government scrutiny is just as important to the work of photojournalists as it is to traditional reporters. Their electronic devices contain vast amounts of First Amendment-protected material. This includes not just photos, video, and writings that may, in the future, be used or incorporated into stories, but also the contents of confidential communications with sources, documents detailing travel plans and expenditures, and large quantities of photos and footage that will never be made public or incorporated into news stories, or that is in the process of being edited.

112. The ability to communicate confidentially with sources is just as important to the work of photojournalists as it is to traditional journalists. A photojournalist's images, footage, notes, documents, and information acquired during the course of covering a story are protected by a qualified privilege in most states. The ability to promise confidentiality is vital to NPPA members' ability to do their work. This is particularly true for NPPA members who routinely interview, capture footage of, or photograph political dissidents, foreign government officials, whistleblowers, victims of human rights abuses, and many others who fear reprisal for speaking to the press.

113. Individuals frequently communicate with photojournalists on condition that their names not be revealed. This includes those who assist photojournalists in developing stories but whose identities and visages are never publicly revealed. It also includes sources who permit NPPA members to photograph or film them on the condition that they will never be identified by name. In many parts of the world, keeping the name of a person photographed secret is enough to ensure that the government and others will be unable to identify and locate them, or that it will not be worth the time and effort.

114. Some sources permit NPPA members to photograph or film them only on the condition that their visual image is blurred or that they are unidentifiable, or that their voice digitally altered. Some NPPA members collect raw footage while covering stories abroad but then, once they return home to the United States, alter visual images, video, or audio they have created about or collected from sources in order to protect a source's identity. Often, NPPA members can only do this alteration work from home in the United States because they need equipment and software beyond what they have on the laptops with which they are traveling.

115. NPPA members do not have the option of traveling without their electronic devices. NPPA members reporting on stories abroad typically require a wide range of electronic devices simply to do their jobs. They must have their still and video cameras to capture images and sounds as well as hard drives, flash cards, memory sticks, compact disks and videotape to store that information. They must bring computers in order to make and store videos, and take and store notes. They must have their laptops and cell phones to communicate with sources, reporters, and the newsrooms or media outlets for which they are working. NPPA members also need their electronic devices with them so they can have access to their own personal records and stay in touch with friends and family.

116. It is unfeasible for NPPA members to avoid carrying information on their electronic devices when they cross the border. Because NPPA members cannot avoid crossing the border with their electronic devices, they must take steps to avoid the harm such a search would cause. When covering a story abroad, when deciding whom to interview, which footage to make, or what notes to take, NPPA members must take into account the likelihood that U.S. border officials may read or copy their interview notes or draft stories; view visual images and footage; or listen to sound recordings they have collected.

117. The ICE and CBP suspicionless search policies undermine NPPA members' ability to guarantee confidentiality to the sources they communicate with abroad. Because ICE and CBP agents may watch, listen to, read, copy, and/or detain the contents of a traveler's electronic devices essentially without limit, it is nearly impossible to promise a source abroad that any images, footage, sounds or documents on the electronic devices with which a photojournalist travels definitely can be kept confidential. The risk that sources' identities will be revealed to border agents – and potentially shared with other parts of the U.S. government or even potentially foreign governments – will lead some sources who otherwise would have shared information, have their picture taken and/or voices recorded or been videotaped to decline to do so.

118. CBP and ICE's claimed authority to detain a traveler's electronic devices for extended periods of time has a particularly negative effect on photojournalists. When CBP and/or ICE detain a photojournalist's camera, laptop, or media storage device, he or she cannot work. CBP and/or ICE's detention of a photojournalist's devices also makes it impossible for them to meet their story deadlines.

119. Because many NPPA members routinely travel abroad with a wide range of electronic devices, NPPA fears that its members' electronic devices will be searched, copied, and detained by U.S. border officials under the CBP and ICE policies.

120. Some NPPA members already have had their electronic devices searched by border officials. For example, NPPA member Duane Kerzic is a freelance photographer who specializes in travel and landscape photography. His photographs have been published in nationally recognized publications and websites such as the *Washington Post*. Mr. Kerzic maintains a blog that serves as his primary method of publishing and disseminating his work.

121. Mr. Kerzic frequently travels for both professional and personal purposes from the United States to Canada and Mexico. Mr. Kerzic typically travels with at least one camera, a laptop, and a cell phone. A large number of Mr. Kerzic's photographs are stored on his camera. Mr. Kerzic also stores a vast amount of both professional and personal information on his laptop, including personal and work-related photographs, email, financial information, stories and blogs he has written, news articles and documents he has read or downloaded from the Internet for both professional and personal purposes, his electronic calendar in which he keeps records of all of his personal and professional appointments, and his web browsing history. On his cell phone, Mr. Kerzic stores photographs, an address book, and some of the approximately 200 text messages he sends and receives every month.

122. In July 2007, Mr. Kerzic was returning to the United States from a trip to Canada. He had been in Canada to, among other things, take photographs for a piece on lighthouses and to take photos of national parks.

123. At approximately 1:30 p.m., Mr. Kerzic arrived at the CBP inspection point at the Thousand Island crossing. Mr. Kerzic was riding his motorcycle. His laptop and camera equipment were in his saddlebag.

124. CBP agents asked Mr. Kerzic where he was going and then referred him to secondary screening. He was asked to wait inside the main building while his motorcycle and saddlebag remained outside, but he stepped outside and witnessed CBP agents going through his personal belongings in his saddlebag and in his motorcycle. A CBP agent noticed Mr. Kerzic was outside and ordered him to return to the waiting area inside.

125. At some point, Mr. Kerzic saw the CBP agent who had been searching his belongings outside walk into the main building in which Mr. Kerzic was waiting. The agent had

Mr. Kerzic's laptop in his hand. Mr. Kerzic saw the agent sit down at a desk, turn his computer on, and peruse the contents of his laptop for approximately 15 minutes. Although Mr. Kerzic typically has his laptop password protected, the password protection was not engaged because the laptop was in hibernate mode. After the CBP agent completed his search of Mr. Kerzic's laptop, Mr. Kerzic was permitted to leave and to enter the United States.

126. As a result of this incident and CBP and ICE's electronic device search policies, Mr. Kerzic changed his password protection settings to ensure that the password is always engaged.

127. Mr. Kerzic fears that his electronic devices will be searched, copied, and detained by U.S. border officials under the CBP and ICE policies in the future. As a travel and landscape photographer, Mr. Kerzic travels frequently across the U.S. border with his electronic devices. To facilitate his work as a photographer, Mr. Kerzic always brings his cell phone, camera, and laptop when he travels. He plans to continue traveling across the U.S. border with these devices in the future. He typically crosses the U.S. border with Canada multiple times per year and the U.S. border with Mexico approximately once a year. He plans to travel to Canada at least once in the upcoming year.

CAUSES OF ACTION

All plaintiffs

128. The CBP and ICE policies violate the Fourth Amendment by permitting the suspicionless search, copying, and detention of electronic devices.

129. The CBP and ICE policies violate the First Amendment by permitting the suspicionless search, copying, and detention of electronic devices containing expressive, protected materials.

Pascal Abidor

130. Searching, copying, and detaining Mr. Abidor's electronic devices violated his Fourth Amendment rights.

131. Searching, copying, and detaining Mr. Abidor's electronic devices violated his First Amendment rights.

PRAYER FOR RELIEF

WHEREFORE, plaintiffs respectfully ask this Court to:

A. Declare that the CBP and ICE policies violate the Fourth Amendment.

B. Declare that the CBP and ICE policies violate the First Amendment.

C. Declare that defendants have violated the rights of Mr. Abidor under the First and Fourth Amendments to the United States Constitution.

D. Enjoin defendants from enforcing their policies of searching, copying, and detaining electronic devices at the international border without reasonable suspicion.

E. Enjoin defendants from searching, copying, and detaining the electronic devices of Mr. Abidor without reasonable suspicion.

F. Order defendants to return all information unlawfully obtained from Mr. Abidor and to the extent information cannot be returned, to expunge or otherwise destroy that information, including photographs and fingerprints.

G. Award the plaintiffs reasonable attorneys' fees and costs.

H. Grant any other relief the court deems appropriate.

Respectfully submitted,

September 7, 2010

Catherine Crump
Speech, Privacy and Technology Project
American Civil Liberties Union Foundation
125 Broad Street, 17th Floor
New York, New York 10004
(212) 549-2500

Melissa Goodman
National Security Project
American Civil Liberties Union Foundation
125 Broad Street, 17th Floor
New York, New York 10004
(212) 549-2500

Michael Price
National Association of Criminal Defense Lawyers
1660 L St. NW, 12th Floor
Washington, D.C. 20036
(202) 872-8600

Christopher Dunn
Arthur Eisenberg
New York Civil Liberties Union Foundation
125 Broad Street, 19th Floor
New York, NY 10004
(212) 607-3300